Multi-parameter Watermarking for Digital Images

Madhusudhan R. V.
Research Scholar
B.M.S.College of Engineering
Bangalore, India

H. N. Suma
Professor and Head
Department of Medical Electronics
B.M.S.College of Engineering

ABSTRACT
The primary focus in today's world is to secure digital images. The digital images are an integral entity in the entire health care management process, from scans to diagnosis to treatment and beyond. While the patient and the doctor(s) are engaged in the process, the digital images of the patient are available and accessible to many. The multi-parameter watermarking enables secure and robust method to enhance the complexity of the system to avert malicious attack. The 'Privacy' of the patient data is enhanced by means of an algorithm with multi-parameter watermarking; the Watermark designed will provide the 'hard-wall' against any unscrupulous attack on the images/system. Implementation outcome will be discussed; algorithm designed and developed to demonstrate a novel watermarking method by defining various parameters for watermarking. Deploying such watermarking methods into tools and procedures will help enhance the 'Privacy' and 'Fiduciary' relationships with which the patient's data is shared between patient and a doctor. It is good to include a combination of methods, visible and invisible watermarks, open and blind watermarks to deceive the unauthorized user or an attacker. Designing the approach which embodies different parameters by using random sequences while the image is sliced with a key unknown to other than the owner (the provider) and actual consumer(s) is critical in providing security to the digital images.

General Terms
Medical Image Security, Watermarking

Keywords
Digital Images, Privacy, Watermarking, Spatial Transform, Frequency Transform, Visible watermarking, Invisible Watermarking, Hard-wall, Fiduciary relationship, Provider, Consumer, Random number.

1. INTRODUCTION
The discussion about 'Privacy' and 'Security' is an integral element in all walks of life today. Privacy of data is of utmost important in one's life for everything that they are engaged. So, Security of data/system from unscrupulous use or attack must be prevented with a robust system. The privacy and security words are used interchangeably, they are two different words, but the intent is same. The use of digital images of patients across the entire process of hospital management system process is a highly complex area/system. The patients' data is used by doctor(s) for arriving at consensus amongst them during analysis, outcome and the treatment. If the system is not robust or trustworthy, the data is under great risk for being used for unknown reasons by many who can have access to the hospital management systems, which will endanger patient's privacy. The intent of introducing secure and reliable watermarks to uniquely identify both the source of an image and an intended recipient after authentication test is passed. Data authentication is one of the most important aspects in each and every tool or system that is used in everyday life. The data is open for an attack; the data manipulation can result in catastrophic outcome in the health sector. The consequences of such malicious use or attack on patients' data have many folds of issues.

A trustworthy and an effective watermarking algorithm must have the following minimum attributes [1]:

Transparency: The embedded watermark in the image should be perceptually and visually imperceptible.

Robustness: A secure watermark should be difficult to remove or destroy, or at least the watermarked image must be severely degraded before the watermark is lost.

Capacity: The watermark capacity includes the discussions and techniques which provide the image with possibility to embed the majority of information.

Different watermarking methods are used and the outcomes in terms of complexity it can provide for any misuse are discussed. The authors presenting a novel watermarking technique and demonstrate a solution to one of the key problems in image watermarking, namely how to hide both visible and invisible watermarks inside grey scale images. The paper is implementing the part of the algorithm proposed as part of [2]. MATLAB 7.10 (R2010a) [3] is used for programming and algorithm implementation.

The patients' chest image is used as an example while the effectiveness of the proposed algorithm is discussed. The paper is deploying spatial transformations, frequency transformations and uses the random key, copyright image and brightness adjustable parameters. With the advent of cloud in all aspects of applications and systems, security of digital images in a cloud environment is very critical. The random functions are used during spatial transformations to include an 'unknown' into the algorithm. The chapter 2 will explain the different watermarking methods used for digital image security and their importance. Using different types of watermarks with different aspects of digital image will create more 'unknowns' to the attacker. The paper establishes the importance of visible and invisible watermarks in order to alleviate the complexity to the algorithm and to the attacker. In chapter 3, the multi-parameter watermarking algorithm is explained to demonstrate its effectiveness. The chapter 4 describes the implementation along with its results. This chapter will conclude with conclusions and future work.

2. DIGITAL IMAGE SECURITY
The digital image of patient needs security in order for us to maintain the privacy of the patient. It is important to device methods to avert malicious attacks. If the attacker is successful, it would be good to show them an incomplete data with image undergoing various transformation techniques to make the digital image very complex to decode upon

unsuccessful authentication. If the tool or the system is able to detect the malicious attack, the purpose to maintain privacy of patient information is achieved.

Three functional components are required in order to embed a watermark. These are: the Image carrier (the original image), a Watermark generator (Multi-parameter Transformation method), and the Watermarked image. Embedding the watermark and detecting it are the main tasks of any watermarking scheme [4]

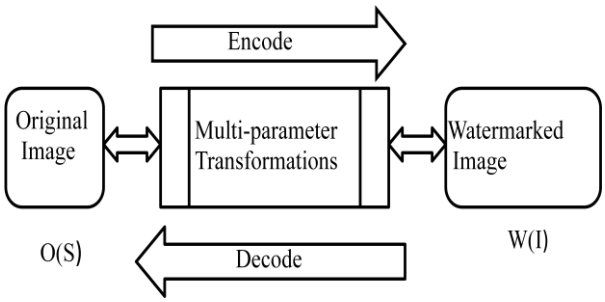

Figure 1. Watermarking scheme

The watermarking scheme is expressed (Figure 1) as:

E[O(S)], W = W[I]

Where, E[O(S)] denotes the original multimedia image/signal (audio, image and video), W is the watermark or the multi-parameter transformations, which contains the information that the owner wishes to embed, and W[I] is the watermarked image or signal. The watermark generator could include various parameters based on the algorithm that is used or deployed.

The decoded information or image must match the original information or image so that there is no slack or loss of information or image. Any slack with regards to patient information will not be appropriate. The watermarking scheme in general can be expressed by: W[O(S), visible-factor, invisible-factor, spatial, frequency,…] = W[I]. The watermarking is a factor of original image O(S), both visible and invisible parameters, and spatial and frequency transformations.

The image carrier or the digital image will undergo spatial transformations to deploy Invisible watermarks [4]. The image is sliced based on the random key generated through rand function; the key is later used in the recovery or the reconstruction of the original image successfully. The key generated will provide the first barrier to the attacker and also the image will be incomplete even if there is an attack, and the system must fail to authenticate.

The digital image obtained after the slice is removed, will undergo transformations to make the image reduced in brightness by factor known to the algorithm/owner, an additional unknown added to the complexity. The multiplying factor used will provide the second additional barrier to the attacker and thereby increases the complexity.

For the visible watermarking, the copyright image is over-laid over the region of interest (ROI). This will potentially create a view to the user that image has been transformed and will likely to focus to attack in the ROI and thereby the invisible watermark will not likely to be under attacker's focus. The other factors considered will get hidden from the attackers focus. The co-ordinates for ROI could potentially be used as other 'unknowns'.

The spatially transformed images are frequency transformed before the images are transmitted. Frequency domain methods mainly include DCT (Discrete Cosine Transform), DFT (Discrete Fourier Transform), and DWT (Discrete Wavelet Transform). DCT provides low arithmetic complexities and bring more robustness to JPEG compression attack and is used in the implementation of the proposed algorithm.

3. IMAGE TRANSFORMATIONS

3.1 Image Planning

A chest image is taken for the implementation of novel digital watermarking, hence-forth termed as the original image O(S). The color image is converted to a gray scale 8-bit image for the transformations. For implementation convenience the zero and ones 8-bit images are created and used for image arithmetic.

As an assumption, the size of the copyright image is smaller than the original image under test. The co-ordinates of the original image are used as the basis for selecting the ROI. The ROI must necessarily make patient's data invisible, the data that is under focus or discussion.

The seed (n) used for creating the sub image is random, the value thus obtained is modulus operated such that it lies in between 1 to 64 for ease of operation. The seed value 'n' can vary depending upon the co-ordinates of the original image.

The Discrete Cosine Transform (DCT) method is used for the frequency transformations

3.2 Spatial Image Transformation

In the spatial domain of watermarking [5-7], the pixels are selected from regions of interest area in the image. The image is modified based on the random number chosen and the copyright that is chosen / desired to embed over digital image. The important factors that provide strength to spatial watermarking are key authentication and its placement, positioning of copyright without altering the digital image content is known as open watermarking. The open watermarking along with 'unknowns' will provide complexity into the algorithm. They bring additional barriers for the attacker and thus attack would pose a real challenge. The operation performed must not diminish the quality of the image.

The algorithms used for spatial watermarking specify the intensity to alleviate the complexity and the 'unknown'. The position of the copyright image will provide both visible and invisible watermark on the digital image of interest. It is necessary to make such algorithms robust by bringing in additional parameters and embedding additional keys within the image coordinates.

The coordinates of the image where the copyright image is embedded, the sub-plane image and the image without the sub-plane are used for watermarking. The seed (n) is used to create (using rand function) the image will add additional complexity to the attacker by increasing the number of unknowns.

The watermark information and along with intensity level multipliers are used to enhance the complexity.

The important aspect that is observed while the research is carried over this aspect, the factors that could alter the original image lies in the imagination of the researcher, the simplicity of the watermarks, complexity to visualize watermark for an unscrupulous user.

3.3 Frequency Image Transformation

The Sub-plane Image O(I) and the image without the sub-plane image O(N-I) undergo frequency transformation before they are transmitted. The DCT is used for the transformations and provides additional invisible watermarks.

The multi-parameter watermarking (Figure 2) will provide the necessary groundwork for the implementation.

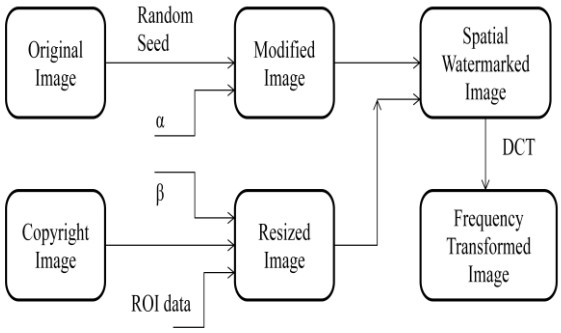

Figure 2. Multi-parameter Watermarking

4. IMPLEMENTATION AND RESULTS

The proposed novel watermarking is implemented using MATLAB and the complexities added to avert attacks on the system are discussed.

4.1 Novel Watermarking discussions

4.1.1 Image Preparation

The Image under test (Figure 3), the original image is read and converted to a gray scale for ease of operation using MATLAB. The original Image O(S) is used for the study and its size is uint8. The zeros and ones Image (the white and black) are used for Image arithmetic. They are needed for Image transformation i.e. to create the sub-plane Image O(I) and the Image without the sub-plane O(N-I). The seed is needed to create O(I) i.e. for column transformation of the original Image using the random key. The rand built-in function is used for creating the sub-plane image. The random number (an 'unknown') will enhance the complexity to attack the image by 'n' times, and 'n' being the maximum value used for column transformation, the complexity is configurable and choosing very high and very low needs to be examined. Higher the value of 'n' increases the complexity for attack.

4.1.2 Spatial Image transformations

The sub-plane O(I) is created using the seed obtained. The entire image is scanned at each column width (with the seed value) and the value at each of the seed co-ordinates is added with a zero image to obtain O(I).

The image without the sub-plane O(N-I) is obtained by subtracting the sub-plane from the original image. The image O(N-I) can be multiplied with a factor (visible watermark – α) to create the visible watermark. The value of α is configurable, is a factor which increases the complexity for the attack. The value of α should be chosen such that the image is not made invisible and it ranges from 1 to 20.

The copyright Image C(S) is chosen such that its co-ordinates are smaller or equal to the co-ordinates of original gray image O(S). In order to overlay C(S) upon O(N-I), the region of interest is critical to hide the information under focus for the attacker. The C(S) is multiplied by a factor (Invisible Watermark – β). The value of β is configurable and can vary from 0 to 1. The C(S) obtained after insertion of β is resized and overlaid upon O(N-I). The copyright image provides both Visible Watermark and Invisible Watermark. The values of the seed, and both α and β adds complexity to the image for the attacker. The spatial transformation (Figure 4) output will have to undergo frequency transformation before it is transmitted.

4.1.3 Frequency Image Transformations

The Sub-plane image O(I) and the image without the sub-plane image O(N-I) undergo frequency transformation before they are transmitted. The DCT is used for the transformations.

The DCT output (Figure 5) will provide high level of security for unauthorized detection and decoding, and low probability of error, complete and easy to understand.

The transmission of O(I) and O(N-I) separately over the network provides open watermarking, it will distract the attacker as both the visible and invisible watermarks are hidden.

5. RESULTS

The co-ordinates of the ROI of the copyright image, the parameters 'seed' value and intensity parameters α and β encompasses different transformation methods. The original image was extracted from basic arithmetic operations without any degradations/slack to the original image. The robustness to the system is included by means of various simple transformations while avoiding complex mathematics, thus time complexity to demonstrate for a large data does not consume large system time. The recovered image and original images do not show any difference after the watermarks are extracted. The recovered image (Figure 3) and its difference with the original image produced a zero image.

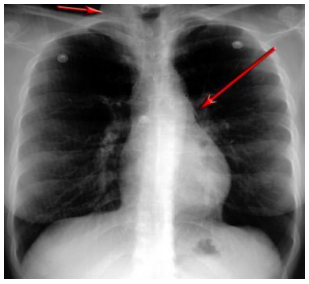

Figure 3. Original Image - Before Transformation

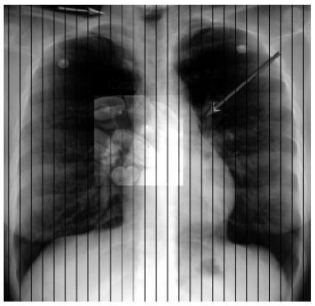

Figure 4. Spatial Transformed Image

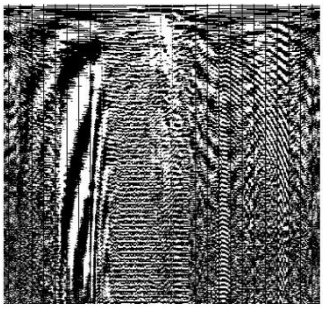

Figure 5. Final Image for Transmission

6. CONCLUSION

The algorithm includes various parameters into the system and thereby creating barriers in decoding the original image or information. The watermarking is simple and deployable and without consuming system capacity. The multi-parameters that are used are variable in nature (as each one provides a range and any number can be picked in random), thus demonstrates greater complexity into the watermark and makes decoding an improbable task.

The seed information and inclusion of auxiliary keys (the private and the public key information) information into the spatially transformed images will enable additional unknowns into the system without creating detrimental capacity issues while the algorithm is easy to implement and deploy.

The copyright image provides both visible and invisible watermarks, is a certain parameter that will deceive the attacker.

The choice of copyright image, its size and placement can provide additional parameters into the algorithm and extends the complexity of the algorithm to a higher degree.

The encryption of the spatially transformed images using RSA with auxiliary keys/parameter, that could be used as an additional proven technology ‘unknown’ into the system [8] to add additional robustness and transparency, without compromising the capacity

7. ACKNOWLEDGEMENTS

Sincere thanks to all the people who encouraged the authors in creating the multi-parameter watermarking, and their valuable insight into the problem, providing attacker perspective, the need for complex watermarks with ‘unknowns’ at each phase of transformations to create a comprehensive and novel watermark. Sincere gratitude is extended to all the reviewers and research scholars for their valuable time in providing valuable feedback and contributions in improving this paper.

8. REFERENCES

[1] Nilchi, Ahmad R. Naghsh, and Ayoub Taheri. "A new robust digital image watermarking technique based on the Discrete Cosine Transform and Neural Network." Biometrics and Security Technologies, 2008. ISBAST 2008. International Symposium on. IEEE, 2008.

[2] RV, MADHUSUDHAN, and H. N. Suma. "A NOVEL MULTI-PARAMETER WATERMARKING SCHEME FOR DIGITAL IMAGES.", Journal of Machine Learning Technologies, ISSN: 2229-3981 & ISSN: 2229-399X Volume 3, Issue 1, 2013, pp.-090-096.

[3] MATLAB from MATHWORKS http://in.mathworks.com/products/matlab/

[4] Suhail, M. A., and M. S. Obaidat. "A robust digital watermarking technique."Electronics, Circuits and Systems, 2000. ICECS 2000. The 7th IEEE International Conference on. Vol. 2. IEEE, 2000.

[5] Song, Wei, et al. "Digital watermarking technique for digital medical images." *Information Technology in Medicine and Education (ITME), 2012 International Symposium on*. Vol. 2. IEEE, 2012.

[6] Chih-Wei Tang, Hsueh-Ming Hang; "A Feature-Based Robust Digital Image Watermarking Scheme". IEEE Transactions on Signal Processing, VOL 51, NO 4, April 2003: pg 950-959

[7] Pik Wah Chan, Michael R. Lyun and Roland T. Chin; "A Novel Scheme for Hybrid Digital Video Watermarking: Approach, Evaluation and Experimentation". IEEE Transactions on Circuits and Systems for Video Technology, VOL- 15, NO 12, December 2005: pg 1638-1649

[8] Beth, Thomas, and Dieter Gollmann. "Algorithm engineering for public key algorithms." IEEE Journal on selected areas in communications 7.4 (1989): 458-466